RELIAQUEST®

Netskope Secure Web Gateway (v2) Integration Guide

Netskope's industry leading security web gateway (SWG) solution enables you to quickly identify and manage the use of cloud applications, regardless of whether they are managed or unmanaged. This integration prevents sensitive data from being exfiltrated from your environment by risky insiders or malicious cybercriminals who have breached your perimeter.

Important: The Netskope Secure Web Gateway (v2) integration will leverage the v2 API permission control, thus providing a different connector than the Netskope v1 API CASB integration. Learn more about the Netskope v1 API connector.

Deployment Type

This integration requires **private cloud** or **vendor cloud** deployments through **port 443**.

If you already know that your organization's environment supports private and vendor cloud deployments, continue with setup. If you are unsure, please work with your internal team to determine your organization's compatibility before continuing.

Required Information and Setup

To integrate GreyMatter with Netskope Secure Web Gateway, collect the following details:

- URL
  - For example, https://reliaquest.goskope.com
- API token

You must also name your Policy URL lists as "RQ Block list" and "RQ Allow list."
See instructions below to gather the required information.

Create a Token with the Required Permissions

Endpoints created previously in the API v2 section (no longer used) will continue to function normally until their expiration date. You will then have to edit, revoke, or delete the endpoint.

Create a Role

1. Within **Settings,** click **Administration.**
2. Click **Administrators & Roles**.
3. Click the **Roles** tab.
4. Select **Create a New Role**.
5. Add a name and description.
6. Select **Administration** in the Permissions tab.
7. Enable and disable the permissions until they match exactly the Permissions table below.
   - **Tip**: Hover over the information icon to the right of a permission to see specific endpoints included in the permission.
8. Click **Save**.

Create the Token

1. Open the **Administrators** tab within Administrators & Roles.
2. Click **Service Account**.
3. Add the **Service Account Name**.
4. Select the role created earlier.
5. Add the duration of the token (the most months allowed).
6. Click **Create**.
7. Click **Copy Token** in the popup and save it somewhere safe for connection with GreyMatter later.

Create two Policy URL Lists

Once you have sent your Customer Success Manager (CSM) or Implementation Specialist your Netskope URL and API v.2 key, follow the steps in the Netskope documentation to create two policy URL lists in your Netskope environment.

- RQ Block list
- RQ Allow list

These policy URL lists must be named ***exactly*** as outlined above for remediation playbook functionality. Please do not edit the list names.

After you create the RQ Block list and RQ Allow list, GreyMatter users can use the playbooks found in the Respond table below.

Permissions and Functionality

Permissions

Use the table below to enable the API permissions and access levels for each GreyMatter capability.

Note: Netskope is rolling out RBAC V3 granular permissions, which require a different set of permissions to be added to the role associated with the API credentials for the connection to GreyMatter to operate correctly.

GreyMatter capability	Action	Required API Scopes
Detect	Get Detection Records	/api/v2/events/data/alert RBAC V3: Skope IT: Alerts: Manage
Respond	Block URL Block IP	api/v2/policy/urllists /api/v2/policy/urllist/deploy RBAC V3: Objects: URL List: Manage and Apply

	Unblock URL Unblock IP	api/v2/policy/urllists /api/v2/policy/urllist/deploy RBAC V3: Objects: URL List: Manage and Apply
	Allow URL Allow IP	api/v2/policy/urllists /api/v2/policy/urllist/deploy
	Unallow URL Unallow IP	api/v2/policy/urllists /api/v2/policy/urllist/deploy RBAC V3: Objects: URL List: Manage and Apply

Respond

Once your integration setup is complete, go to the Respond tab in GreyMatter and use the variables below to test the various playbooks.

Playbook Name	Description	Required Input Variable(s)
Enrich List	Enrich Policy URL List	URL List Name Example: RQ Block List
Allow URL	Adds url(s) to a URL list found in Netskope Customer Admin Dashboard under Policies > Profiles > Web > URL lists. The URL list will be added to Custom Categories (by using the Admin user) as an include list in order to function properly.	URLs Example: www.test.com *Separate multiple values with commas.
Unallow URL	Removes url(s) from a Policy URL list found in Netskope Customer Admin Dashboard under Policies > Profiles > Web > URL lists. The URL list will be added to Custom Categories (by the Admin user) as an exclude list in order to function properly.	URLs Example: www.test.com *Separate multiple values with commas.
Block URL	Adds url(s) to a URL list found in Netskope Customer Admin Dashboard under Policies > Profiles > Web > URL lists. The URL list will be added to Custom Categories (by using the Admin user) as an include list in order to function properly.	URLs Example: www.test.com *Separate multiple values with commas.
Unblock URL	Removes url(s) from a Policy URL list found in Netskope Customer Admin Dashboard under Policies > Profiles > Web > URL lists. The URL list will be added to Custom Categories (by the Admin user) as an exclude list in order to function properly.	URLs Example: www.test.com *Separate multiple values with commas.
Block IP	Adds IP(s) to a URL list found in Netskope Customer Admin Dashboard under Policies > Profiles > Web > URL lists. The URL list will be added to Custom Categories (by using the Admin user) as an include list in order to function properly.	IP Example: 1.1.1.1 *Separate multiple values with commas.
Unblock IP	Removes IP(s) from a Policy URL list found in Netskope Customer Admin Dashboard under Policies > Profiles > Web > URL lists. The URL list will be added to Custom	IP Example: 1.1.1.1 *Separate multiple values with commas.

	Categories (by the Admin user) as an exclude list in order to function properly.	
Allow IP	Adds IP(s) to a URL list found in Netskope Customer Admin Dashboard under Policies > Profiles > Web > URL lists. The URL list will be added to Custom Categories (by using the Admin user) as an include list in order to function properly.	IP Example: 1.1.1.1 *Separate multiple values with commas.
Unallow IP	Removes IP(s) from a Policy URL list found in Netskope Customer Admin Dashboard under Policies > Profiles > Web > URL lists. The URL list will be added to Custom Categories (by the Admin user) as an exclude list in order to function properly.	IP Example: 1.1.1.1 *Separate multiple values with commas.

Investigate/Hunt

GreyMatter queries against alerts of netskope.
Default limit: 4 calls/second

Detect

Netskope Secure Web Gateway supports **Detection at Source.**

Note Syncing and **State Syncing** are *not* supported for **Vendor-Authored detections.**

Disclaimer: All customer data is classified and handled as 'Confidential' (as outlined in our Data Classification & Handling Policy). Customer data is restricted to authorized personnel only based on their business need. ReliaQuest uses least privilege and role-based access controls via Active Directory to provision and manage access. Please see our Access Control Policy for more information. ReliaQuest employees are also required to sign confidentiality agreements as part of their employment.